Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures

Ola Aleksandra Michalec, Dirk van der Linden, Sveta Milyaeva, and Awais Rashid, *University of Bristol*

https://www.usenix.org/conference/soups2020/presentation/michalec

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

Open access to the Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Industry Responses to the European Directive on Security of Network and Information Systems (NIS): Understanding policy implementation practices across critical infrastructures

Ola Michalec
University of Bristol

Dirk van der Linden
University of Bristol

Sveta Milyaeva
University of Bristol

Awais Rashid
University of Bristol

Abstract

As traditional legacy systems that run critical national infrastructures (CNI) are increasingly digitized for performance monitoring and efficiency, significant attention has been brought to improving their cyber security. Network and Information Systems Security (NIS) Directive is the first European-scale attempt to establish a high standard of cyber security among CNIs. NIS raises questions about defining scope, providing evidence or mobilizing funding. Most importantly, there is the fundamental question whether it would become a tick-box exercise or lead to long-term improvements in security practices. We interviewed 30 cyber security practitioners in the UK to gather an in-depth understanding of NIS implementation and its probable futures. Our analysis found that the emerging field of Operational Technology Security is yet to formulate norms, standards and career trajectories. We are, therefore, at a critical junction, where the scope of the profession is shaping together with the need for evidence-based policy advice. Our findings are twofold: (1) a number of security tropes (e.g., "security solutions are the same across the sectors"), which may drive implementation of regulations such as NIS; (2) a classification of cyber security practices mapping the diversity of policy interpretations. We conclude with recommendations for policymakers and CNI operators.

1 Introduction

Critical National Infrastructures (CNIs) are facilities and systems essential for a country to function. While the exact scope is up for a political decision, sectors like water, energy, transport, defense, health, emergency services would typically be designated as CNIs. However, not all components of these sectors are deemed critical, for example, current policy advice focuses on protecting systems where a major detrimental impact on the delivery of services could pose serious threats to human life or compromise national security [31].

Critical infrastructures are supported by the Operational Technology (OT) and Information Technology (IT) systems. Some examples of IT systems are billing software, staff intranet or data servers, however, their criticality depends on the organizational context. Meanwhile, OT is defined as hardware and software used to monitor and control physical equipment like pumps or valves [24]. Some example systems and devices used in OT environments include: *1) Supervisory Control and Data Acquisition (SCADA)*: control network architecture used for monitoring assets over large geographical areas; 2) *Programmable Logic Controllers (PLC)*: industrial computers built to endure harsh conditions and provide strong safety and real-time properties; 3) *Telemetry, or sensors communicating using radio, infrared or cellular networks*; 4) *Actuators*, components which drive the actual physical process based on commands from PLCs. Experts working in the Operational Technology environment would typically have an engineering background, with specialization in control, networks or safety processes. In the absence of university education, OT specialists would progress in their careers starting from blue-collar roles like technician and plant operator [48].

For decades, OT systems have been limited to basic functionalities, however, with increased digitization and the advent of the Industrial Internet of Things (IIoT), they modernize at an unprecedented scale. One of the reasons for the slow pace of technological advancement in Operational Technology is the strict regulatory environment of the critical infrastructure operators which prioritizes safety. However, the most recent generation of OT devices promises not only improvements in safety but also efficiency and monitoring, e.g., automatic leak detection in water systems or increasing flexibility of energy networks [15, 18, 23]. Yet, reports of recent attacks on critical infrastructures show that securing OT systems from cyber

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

attacks still remains a challenge (see analyses of Triton [29] and the Ukrainian power grid attack [21]).

OT security is much younger than its IT counterpart, and its concerns, traditions and feasible solutions cannot exactly translate from IT security due to the differences in material and regulatory arrangements. Furthermore, a significant knowledge gap exists in terms of OT cyber security best practices [74]. Although the differences between OT and IT security are still poorly understood, protecting Operational Technology environments is a priority for nation-states due to their strategic importance and role in delivering essential services [19]. Therefore, the regulations and standards informing the design of OT systems require special attention from security researchers and practitioners.

In order to investigate the interactions between regulations and innovation, we turn to the Network and Information Systems Security Directive (NIS). NIS is the first European-scale attempt to regulate and stimulate the development of cyber security in CNIs [2]. The directive asked each complying government to identify sectors in scope of the policy. The designated industries are considered essential to human life and exposed to cyber security incidents. As such, there is a number of Operational Technologies within the scope of NIS, which have not been previously dealt with by other digital regulations (i.e. General Data Protection Regulations).

The development of new regulations in the field of emerging technologies raises questions about defining scope, providing appropriate evidence, mobilizing funding and, finally, implementing policy [25]. Consequently, two questions about the possible futures of NIS need to be answered:

- What responses to NIS are likely to bring about meaningful organizational change?
- How can NIS avoid being reduced to a *tick-box exercise*?

While we cannot predict the future, we can anticipate a range of potential outcomes by investigating how OT security practitioners gain their expertise, and how they then apply it to policy interpretation and implementation. We interviewed 30 cyber security practitioners based in the United Kingdom, asking about their experiences of the evolving cyber security policy landscape in the context of critical infrastructures. The research project was guided by the following questions:

RQ1. How is the knowledge of OT security created?

RQ2. How do CNI operators interpret and implement cyber security regulations?

RQ3. What OT security practices can be observed as a result of these regulations?

We addressed the above questions in the context of NIS Regulations, as implemented in our case study country, the United Kingdom. Our questions were motivated by the interest in the emerging profession and the act of collective "sense-making" of the unprecedented policy. We argue that only by understanding the practitioners and practices on the ground we can establish whether and how security may be advanced as a result of regulations such as NIS. Our work is among the first to investigate organizational and practitioner responses to NIS. The novel contributions of our work are as follows:

We identify four Operational Technology (OT) *security tropes* which could influence the implementation of OT security regulations: "separation means security", "IIoT is inevitable", "security solutions are the same across the sectors", "raising awareness leads to security". In these four tropes encountered, the notion of cyber security was equated with solely individual or technological capability. We propose that organizational and political dimensions of security should receive its due regard in the debate. Our analysis of these tropes acts as a call to shape the trajectory of professionalization in this field. We recommend that practitioners who encounter OT security tropes should seek robust evidence and ensure that these statements are appropriately translated to the OT and sector-specific context before being circulated.

We propose a classification of Operational Technology cyber security practices which maps the diversity of policy responses and interpretations. We analyze these practices in conjunction with OT security tropes to indicate how practitioners' understanding of NIS could lead to more security or more insecurity. In doing so, we provide a set of recommendations for policymakers and critical infrastructure operators. Finally, we set the agenda for further research on the emerging field of OT security.

2 Related Work

2.1 (Supra)national policy or legislation on CNI cyber protection

Directive (EU) 2016/1148 [2] on establishing a high level of security of Network and Information Systems (NIS), commonly referred to as the "NIS Directive", is the European Parliament's effort to improve network and information systems security across the European Union (EU). The NIS Directive has been mentioned as a motivating factor for organizations to improve their cyber security processes (cf. [5,47]). At the time of writing (June 2020), most governments identified the policy scope, outlined implementation road maps and suggested penalties for non-compliance [10,51].

Significant research has been done on other European efforts in unifying law addressing digital infrastructures, such as the General Data Protection Regulation (GDPR) [28,39]. However, despite the importance of critical infrastructures to society, organizational and practitioner response to NIS have so far not been investigated in depth. Maglaras et al. [49],

for example, gave a detailed overview of challenges for the implementation of the NIS Directive in Greece, but little work since then has explored practitioners' experiences of policy implementation since different member states transposed the directive into their respective legislations.

Meanwhile, in our case study country, the UK, Shukla, Johnson, and Jones [64] discussed how NIS implementation strategy addresses critical infrastructure security risks in the UK, giving a set of ten recommendations to bridge gaps identified in the NIS framework. Their suggestions centered around holistic security governance, outcome-based audit approach, and progressive road map to improve cyber capabilities of the critical infrastructure operators.

Overall, the UK is considered to be fairly mature in terms of IT cyber security, and less so when it comes to the OT systems [64]. The government's ambition is for the UK to grow domestic cyber security sector and become the global cyber security leader [20]. The potential to realize these ambitions will depend on the governance arrangements across critical infrastructures. Carr [19] called for sustained attention on the emerging public-private partnerships between the operators and the government's regulatory bodies. Each of these partnerships could impact the trajectory of NIS implementation due to varying relationships and funding arrangements between the (energy, water, transport) operators and regulatory bodies overseeing equipment safety and pricing regimes.

Finally, in contrast to Shukla et al., our work presents one of the first empirical works performed during the implementation of NIS, going into much more granular detail to the challenges faced by those affected by NIS, allowing us to reframe what advice remains most urgent to practitioners.

2.2 Security Practices and Behaviors

While researching policy documents is crucial to investigating cyber security regulations, implementation is ultimately a social activity. After all, people create shared understanding of secure behaviors and practices. Previous research on human factors in cyber security focused on systematizing the types and kinds of security behaviors. For example, there is the mapping of employees' information security behavior to various levels of information security knowledge [3]. A typology of end-user security behavior triggers is suggested, where social triggers (i.e. interacting with, or observing other people) are the most common types, and social interactions in the context of security are essential to our understanding of security-related behaviors [26, 27]. Risk perception may also play a role in security practices, as incorrect perceptions have been noted to play a significant part in past attacks on CNIs [57]. Such incorrect perceptions may arise due to latent design conditions, or improper specification of system qualities, borders, observability and controllability [33], making it difficult to reduce blame to the level of the individual. Furthermore, it is necessary to investigate the motivators and barriers of employees' security behaviors, paying attention to responsibility, personal and work boundaries and how these differ across various contexts [12]. To stimulate security behaviors, people need to be positively motivated, e.g., by overcoming negative perceptions of security through establishing trust with audiences and addressing concerns in an honest, transparent way [37]. Moreover, it would seem that one-size-fits-all solutions to improving security are not necessarily realistic, as different authentication methods place burdens on their users, leading to great variations among participants' security approaches and implementations [50].

We argue that the response to cyber security regulations is a result of mutual shaping between policy interpretation, capabilities of the stakeholders and material resources available [63]. Positioning the research in the social rather than individualistic framework requires a shift from behavioral theories to the theories of practice [72]. Situated practices are "routinized and hierarchically organized human activities which take into account material resources" [62]. Although they are widely studied in IT and engineering [30, 71], Cavelty's interdisciplinary literature review [22] shows that situated practices have received limited attention in cyber security. The practice lens encourages to trace how tacit knowledge, circulation of norms and evolving technological capabilities influence each other to shape "what people do" and "how people are". Finally, this focus emphasizes that "security best practices" found in industry guidelines and regulations, when performed in the real-world context, can sometimes lead to the unexpected instances of insecurity [22]. For this reason, it is crucial to understand the difference between "best practices" on paper (i.e. in NIS guidelines) and situated practices found during policy implementation process.

2.3 Differences between IT and OT security

As typical information technology (IT) and operational technology (OT) solutions differ in hardware and software, securing them necessarily does so too. The protection of OT systems from cyber attacks is increasingly important [38, 69]; below we outline how the typical concerns and favored solutions in OT systems differ from the IT (Table 1). It is worth noting that OT security measures are not as established as IT measures, therefore, their efficacy is still under debate [46, 56].

Security behaviors in OT systems may thus also be an entirely different beast from IT systems, as the varying demands of different stakeholders represent many complexities that place OT security into a gray area, with security workers having to balance competing and complex demands [74]. CNIs which fall under NIS operate both OT and IT systems. This further emphasizes the need to study differences between the security practices in IT and OT context, so that we understand what support practitioners require.

Table 1: Differences between IT and OT systems and typical security measures ([46, 56]).

IT SYSTEMS	OT SYSTEMS
• State of the art technology • Usually private enterprises • Priorities are: confidentiality, integrity and availability • Operated by office-based IT professionals	• Legacy systems • Highly regulated for safety, mix of private and state-owned organizations • Priorities are: safety, reliability, robustness, maintainability, integrity and availability • Operated by engineers and manual laborer's
IT SECURITY	**OT SECURITY**
• Relevant standards: ISO270001, NIST Cyber Security Framework • Common solutions: pen testing, firewall, antivirus, insurance, access management • Behaviors and practices well documented	• Relevant standards: IEC 62443 • Potential solutions: patching, access management, firewall • Behaviors and practices poorly understood

3 Study Design

We performed a qualitative study using key informant semi-structured interviews [44] between November 2019 and January 2020, interviewing 30 people across professions and sectors to provide opinions and experiences of security in critical national infrastructures (CNIs). The study was approved by our institutional review board.

3.1 Recruitment

We used a combination of snowball sampling [55] and purposive maximum variability selection [52] attending industry events to establish contacts (10 participants), and through there expanding our search to mutual contacts (17 participants). Besides this, we identified a small number of participants (3 participants) through online cold calling. Our informants were cyber security practitioners who are currently working in various CNI sectors. We stopped recruiting when we reached a sufficient variation of sectors (e.g. energy, water, transport) and roles (e.g. regulators, security consultants, CNI operators) as well as data saturation, a point where consecutive interviews cease to provide novel insights [32]. A basic overview of the participants we recruited is given in Table 2.

3.2 Interview design and methodology

We used a common topic guide for the interviews, shown in Table 3. We designed the topic guide to allow gradually building a rapport and make participants comfortable (interview questions 1-3 in Table 3). In particular, interview questions 2 and 4 pertain to RQ1; interview questions 5 and 6 relate to RQ2 and interview questions 3 and 7 are relevant to RQ3. Questions were tailored to each participant to account for differences in sectors and professions. Interviews took place either at the participant's organization, our institution or via online calls. One primary researcher conducted all interviews,

Table 2: Demographic data.

#	Role	Sector(s)
P01	Security consultant	Oil and Gas
P02	Regulator	Energy
P03	Regulator	Energy
P04	Security working group co-ordinator	Energy
P05	Engineering consultant	Energy
P05	Engineering consultant	Energy (Civil Nuclear)
P07	Director in Engineering consultancy	Water, Energy (Civil Nuclear)
P08	Security Manager at the CNI Operator	Energy
P09	Security Trainer	Defence
P10	Incident Response Director	IT, Finance
P11	Security consultant	IT, Finance
P12	Vendor of security product	IT, Finance
P13	Lawyer	IT, Finance
P14	Working group coordinator	Telecoms
P15	IIOT Manufacturer	Across all
P16	Security consultant	Across all
P17	Business Development at IIOT R&D	Across all
P18	Project Manager in Engineering Consultancy	Across all
P19	Project manager at IIOT R&D	Across all
P20	Security consultant	Transport (Rail)
P21	Safety Engineer	Transport (Rail)
P22	Human factors expert in Engineering Consultancy	Transport
P23	Incident response for a manufacturer	Transport
P24	Security Consultant	Water
P25	Security Consultant	Water
P26	Security manager at the CNI operator	Water
P27	Security manager at the CNI operator	Water
P28	Regulator	Water
P29	Regulator	Water
P30	Regulator	Water

which was necessary to build up rapport and trust given the sensitive nature of participants' work, and to allow for snowballing recruitment. Each interview lasted approximately 60 mins; all conversations were recorded with the interviewees' consent. No reimbursement was given for participation.

3.3 Data coding and analysis

Interviews were transcribed using a professional service. Transcripts were subsequently coded using NVivo software. The coding was based on thematic analysis according to Braun and Clarke [16], taking an inductive, open approach, meaning that we established our themes and sub-themes based

Table 3: Topic guide.

Topic guide for semi-structured interviews
1. *Story of OT security in your sector/organization*: How did OT security look like before NIS, what has NIS changed in comparison?
2. *Story of your career*: How did you get into security? How did your previous roles influence your current job?
3. *Situating security in a sector-specific context*: What are the typical security concerns, regulations, technologies and procedures in your sector/organization?
4. *Standards and regulations*: How do you apply industry standards and security policies in your organization? How to ensure they are applied successfully?
5. *Experiences from NIS*: How do you understand NIS guidelines? What are your opinions on it? How have you been implementing NIS so far?
6. *Investments and innovations in your organization/sector*: What are your plans for the next few months/years with regards to improving security? How will NIS influence your future investments?
7. *Communicating OT security in your organization/sector*: How should we communicate across IT-OT divide? How should we communicate between the board members and the technical experts?

on the most frequent and novel responses rather than fitting participants' opinions to pre-designed categories. We iteratively discussed the transcripts and the developing coding schemata, where we focused on fostering discussion among the authors and building towards a shared understanding of the coded data to ensure coding quality [42]. As Barbour [7] notes: "the degree of concordance between researchers is not really important; what is ultimately of value is the content of disagreements and the insights that discussion can provide for refining coding frames." While some categories were descriptive (e.g., notes on participants' backgrounds and sectoral differences in NIS implementation), in most cases, the act of coding reflected our analytic efforts (e.g., we coded participants' ways of talking which reflect IT, engineer's or regulator's "worldviews"). The resulting codebook is given in Appendix A. We grouped repeating and widely occurring responses to represent major themes (security tropes and policy implementation practices) as well as their sub-themes. For example, "Security tropes" were referenced 102 times across 23 participants, while policy practices were referenced 246 times across 25 participants. We noted that "security tropes" was a worthy category of analysis, as it reflected the emerging state of Operational Technology expertise. Similarly, we classified "policy implementation practices" to establish an exploratory categorization system so further researchers of NIS and other security policies could verify it against their empirical findings.

3.4 Limitations

While we built a sample to ensure the validity of our research (e.g., aiming at our sample being representative in terms of sectors, roles and professions), we neither intend, nor claim to offer highly generalizable results. Although the sample includes a range of people, sectors, and professions, the insights derived from the coding do not necessarily generalize to any of those variables, nor to the wider critical infrastructures context. Nevertheless, the paper provided unique insights into NIS and its implementation. Due to the sensitive nature of the field, an important and time-consuming part of the recruitment process focused on gaining trust and access to participant's honest thoughts and reflections. This was partially enabled by the authors' participation in an industrial-academic research consortium, which may have influenced the topics participants were willing or prioritized to talk about.

4 Results and Discussion

In summary, our research found that the emerging field of Operational Technology Security is yet to formulate professional norms, qualification certifications and career trajectories. We are, therefore, at a critical junction, where the future of the profession is shaping together with the urgent need for evidence-based policy advice, such as NIS directive. Our findings are twofold: (1) a number of security tropes, common practitioners' generalizations about the best OT security measures (e.g., "security solutions are the same across the sectors"); (2) a classification of cyber security practices mapping the diversity of policy implementation (e.g. negotiation, workarounds) . We analyze these practices through the lens of security tropes to highlight whether they are likely to bring about or hinder organizational change with regards to security best practices. In doing so, we provide a set of recommendations for policymakers and CNI operators.

The following section analyzes the results in detail. We first provide a demographic description of participants and outline our findings on the professionalization of Operational Technology security. Then, we analyze the four security tropes widely discussed in the context of NIS implementation. Finally, we propose a classification of policy implementation practices and illustrate how they could lead to security or insecurity. Combining results and discussion demonstrates how a direct dialogue between empirics and theory can advance the field of Operational Technology security as a whole.

4.1 New regulations, new roles

NIS itself mobilized the OT security expertise, with new roles created to enable implementation of cyber security policies. For example, all 5 regulators joined their organizations no earlier than 6 months before the interview date. We observed that some participants anticipated that future recruitment might prove difficult as "*one of the biggest challenges is to scale up resources and to go to the market, especially in OT. There is a really, really, really, really limited number of specialists*" [P03]. Therefore, we argue that NIS both *creates the skills gap*, by prioritizing the need for a new type of expertise as well as *fills the gap* by unlocking investment in new staff.

According to our participants, OT cyber security is a relatively new concept: during the interviews participants frequently remarked that they *"worked in cyber security back*

when there was no such thing as cyber security" [P27]. To understand how participants' professional experience built their present expertise, we charted the diversity of informants' backgrounds in Figures 1 (length of relevant experience) and 2 (education). In the absence of OT security-specific degrees, participants often studied computer science, information security or engineering. In terms of professional experience, interviewees' past roles were largely technical, with only 4 participants having at least 3 years of experience in human and social aspects of technology.

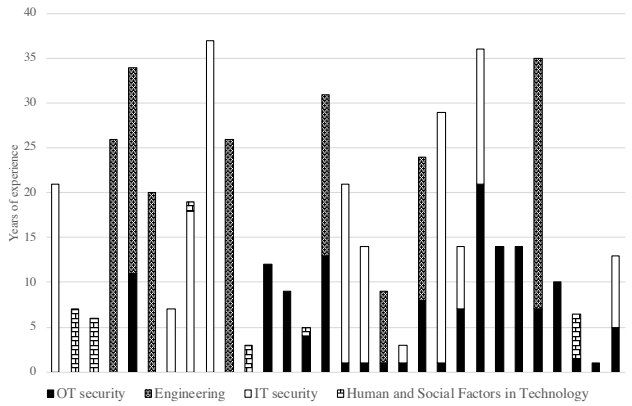

Figure 1: Length of relevant experience – each bar on X axis represents a participant. Y axis corresponds to the cumulative years of relevant experience. X axis is anonymized, and participants are represented in a random order.

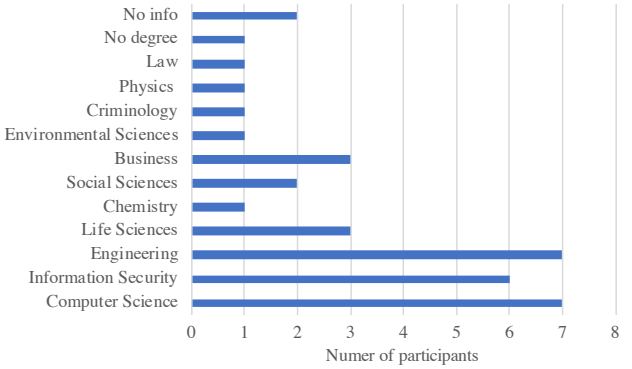

Figure 2: Participants' education. N.B. Some participants obtained more than 1 qualification.

Despite the burgeoning of accreditations and certifications, some participants remain skeptical about their value: *"You look at an individual course and that might be $6,000, and then you realize that's only a small part of it and you need another seven modules, so that ends up $40,000 for a certificate. Should you be spending that much money on certification or should you be going out and helping the industry in doing better and learning more?"* [P16]. Drawing from participants' skepticism about the current cyber security education, we contend that the pathway to professional recognition is not clear.

Across the participants' pool, we observed considerable lateral movement across CNI sectors (e.g., from water to energy), with 24 participants working for more than one CNI sector in their careers. In particular, the defense sector was a notable employer of security experts, as it features in the working history of 8 interviewees. More than half of participants (18) moved across organization types (e.g., from the private sector to the public sector). This could partially explain reports on the OT professionals shortages [40], where the skills gap is shifted from one sector to another rather than tackled with a systematic effort to train new professionals.

4.2 OT Security Tropes

Our main finding suggests that the state of OT security professionalization observed at the time of data collection is characterized by a combination of the following factors:

1. Increasing pressure to recruit experts;
2. Lack of established and "typical" career trajectory;
3. A need for professional education and guidelines.

As the question of NIS implementation is positioned in the center of this "trilemma", we risk that poorly evidenced and OT-inappropriate advice will be circulated to influence key security decisions.

We examined the instances where participants discussed OT security tropes. We define them as widely held beliefs which require a further level of detail before they can be successfully applied to the OT context. Due to the combination of rhetorical qualities like generalization, ambiguity and strong normativity, they lead to the creation of advice which can be easily marketed at mass scale [9]. As they're quite vague, they can appeal to professionals from diverse backgrounds. We argue that participants held a variety of opinions on "the best OT security practices". This reflects the diverse levels of sophistication when it comes to practitioners' understanding of organizational, social and political contingencies of NIS implementation. As the social science studies of expertise suggest, it is crucial to understand these tropes in order to aid professionalization of the industry and effective policy implementation [61].

As previous research on cyber security expertise demonstrated, "translating" security knowledge form IT to OT is not only a matter of IT experts learning engineering [70]. We first ought to enquire: who believes in these tropes and why? Then, we ought to pay attention to people and organizations

benefiting from the circulation of OT security tropes by asking: who makes a profit of it? Whose security "solutions" fit the stereotypes? Finally, we should bear in mind: what other measures are overlooked as a result?

4.2.1 Separation means security

Interviewees discussed the feasibility of security measures. In particular, "air-gapping" received considerable (both positive and negative) attention. Air-gapping employs physical separation of secure computer networks from the unsecured ones (e.g. public Internet, local area network). Traditionally, air-gapping has been applied to critical infrastructures due to the low level of digitization prevalent among their OT systems.

However, the current state-of-the-art attack methods are sophisticated enough to deal with air-gapped systems, with the most well-known (at least to the security practitioners) example being Stuxnet [59]. Yet, outside the OT security bubble, the conversations could look different, e.g., one of our participants recalled difficulties when convincing senior management that "air gapping" does not ensure security: *"When you're talking to the board and they say, "We don't need to worry about security because our production facility is air-gapped", there is only one place which is air gapped and that is Battlestar Galactica!"* [P01].

Debunking air-gapping is justified not only with the advancements in threats, but also with participants frequently predicting that OT systems will continue to become more IT-like, for example through implementing IT-standard network protocols in OT devices or migrating data to the Cloud. Although technologically feasible, IT-OT blending is not adopted across CNI sectors at the same rate due to the current regulatory constraints, such as the requirement for the OT equipment to comply with industry *safety* standards. For example, the regulator for the water industry debunked an assumption of widespread digitalization across all critical infrastructure sectors: *"There are a small number of products that have to be approved because they're in contact with drinking water. For instance, a valve with a computer on the back of it. It's not worth approving this valve with the new computer so you have to use the old computer"* [P28]. In the same interview, he later argued that if the safety regulations remain stringent, OT systems will likely stay, to some extent, air-gapped, meaning *"ultra-safe old-school where you don't connect anything"* [P28]. We, therefore, recommend that before falling for the most technologically advanced (and the most expensive!) security advice, CNI operators ought to sense-check it against the organization-specific conditions. Figure 3 demonstrates how this "trope" relates to NIS.

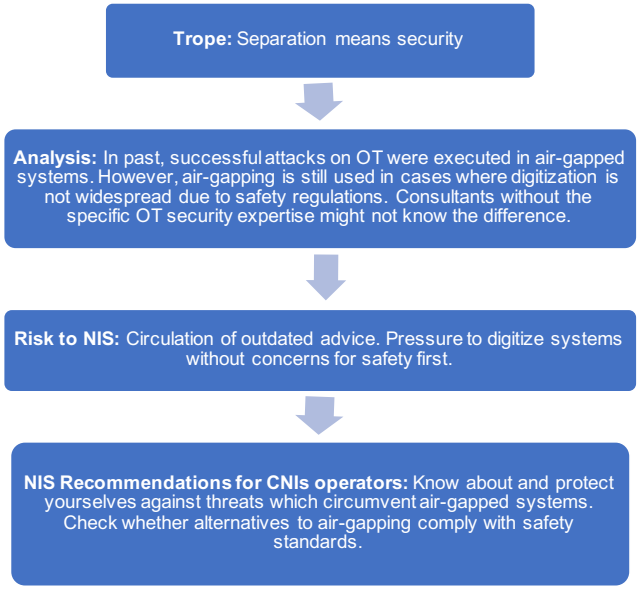

Figure 3: Analysis of the OT security trope: Separation means security.

4.2.2 IIoT is inevitable

Tracing the course of innovation further, we observed a paradox where as many as 11 interviewees would express worry about IIoT, yet at the same time would say it's "inevitable". We observed various ways to contribute to pervading the discourse of "the IIoT inevitability": from framing OT cyber security as a challenge to be overcome solely with technical solutions to treating the socio-political complexities of IIoT as irrelevant to the participant's job. Boyd and Holton [14], in their analysis of innovation discourses, critiqued the assurances of "inevitability". They called for an alternative perspective emphasizing complexity, uncertainty and the role of power relations. As such, we recommend that an alternative look at the future of IIoT would ensure that concerns about security, privacy, affordability, sustainability and labor losses are jointly addressed before deciding whether and how IIoT will be present in critical infrastructures.

In terms of NIS implementation, participants flagged a misalignment between the timescales of IIoT innovation and policy development: *"We're facing the problem of IIoT arriving. When we did the self-assessment, everyone was using very traditional industrial control systems. In that time in the last six months, we've all started adopting IIoT and it's going to get worse. So, it's a big change and it's one that's very much on everyone's radar including mine"* [P26]. We argue that although this is certainly a concern to the industry, concerns about IIoT also opens up a space to generate critical inputs into the evolving OT security regulation landscape. Given that innovation is not technologically determined but

it's a result of co-production, mutual shaping between the society and technology [54, 63], security practitioners are key stakeholders in the process of IIoT co-production as they have the agency to raise, publicize and prioritize their concerns. Figure 4 demonstrates how this trope relates to NIS.

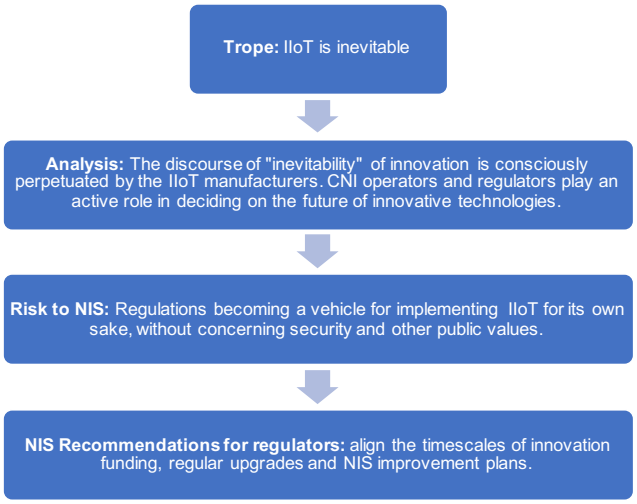

Figure 4: Analysis of the OT security trope: IIoT is inevitable.

4.2.3 Security solutions are the same across the sectors

Another techno-deterministic understanding we observed among participants is that security solutions do not differ across the CNI organizations because *"the tech basis of cyber is the same across the sectors"* [P09]. However, a closer look at the CNI operators' arrangements reveals cross-sectoral differences which can be explained by physical constraints and governance traditions, e.g., *"In oil and gas is, the production facilities, be that an offshore oil platform, are in a small geographical location, you can't get onto an offshore oil platform without getting on to a helicopter. Oil or gas pipelines, on the other hand, are more like the electricity grid, but they are run and owned and operated by completely separate companies. In the water industry, we are unique in so far as we operate both the production sites and the distribution network, and the security model is very different for the two"* [P26].

The diverse ways practitioners understand the application of security measures in new contexts raises questions about the biases they might carry when working across CNI sectors or across IT and OT systems. If security is a subject to the material [4] and regulatory [53] constraints, what is the efficacy of sharing "best practices" or even a cross-sectoral top-down directive like NIS? We recommend that initiatives focused on sharing "best practices" should go beyond talking about security measures and take time to explain unique organizational contexts. We hope that, by turning to the diversity of participants' experiences, we will able to exemplify the need for contextuality in OT security policy development. Figure 5 demonstrates how this trope relates to NIS.

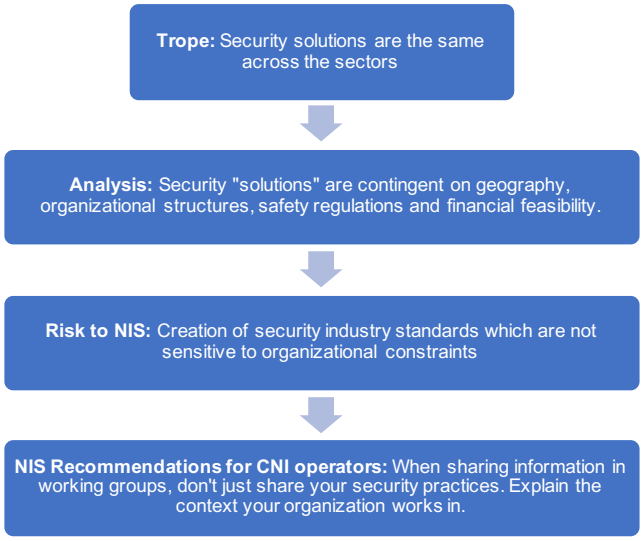

Figure 5: Analysis of the OT security trope: Security solutions are the same across the sectors.

4.2.4 Raising awareness leads to security

Mentions of "awareness raising" were present in 15 interviews. Participants frequently acknowledged lack of awareness as a key issue in OT Security. They had diverse understanding of what constitutes good "awareness" and the likelihood of awareness leading to improved protection. While staff training is one of the deliverables of NIS, we problematize "raising awareness" as an effective educational activity and encourage practitioners to gain a more nuanced understanding of human and organizational factors. The concept of "awareness raising" has gained popularity through the application of the "information deficit model" since the 1980s [65]. The core tenets of the information deficit model are: 1) Ignorance is the reason for a lack of support for various issues in science and technology; 2) Better awareness of science and technology will lead to the desired societal outcomes (ibid.). The framework has been discussed in several empirical studies of cyber security [6, 36, 75]. Information deficit model received criticisms for proposing that rational and individual agency is the key determinant for a given action. However, in the words of an OT Security Consultant, "raising awareness" might not only fail to bring about positive results, but also unwittingly deteriorate the state of affairs: *"P24: I believe is that OT cyber security is such a new thing. It's in the minds of academia and it's in the minds of certain people within essential operating companies. It is not disseminated into the public awareness either as an employee or as a member of the public. And it shouldn't be because general population*

can't rationalize. They can worry. So why would you want to worry a population? Is it beneficial for society to know of all the things that bad people want?"

Going back to the notion of staff training as "raising awareness" of NIS, we found that OT experts had a range of opinions in terms of evidencing that training would work: from colleagues' anecdotes, own reviews, to, finally, an increase in security tickets. In particular, the third notion deserves more attention: one CNI operator reported that although staff training successfully raised awareness about security, it looked like a failure from the outside as it led to an increase in security incidents being reported. We recommend that for OT security, the goal of "raising awareness" ought to be reframed to consider the following questions. First, how do you evidence awareness and security? Second, who should be aware: IT experts, engineers, board members, manual workers, policy makers or the general public? Third, what should they be aware of: technologies, politics, human factors, organizational issues? Finally, we recommend that "awareness raising" should be combined with other training methods, e.g. linking security measures to personal values or communicating operational benefits of security (e.g., improved monitoring, and asset management). Figure 6 demonstrates how this trope relates to NIS.

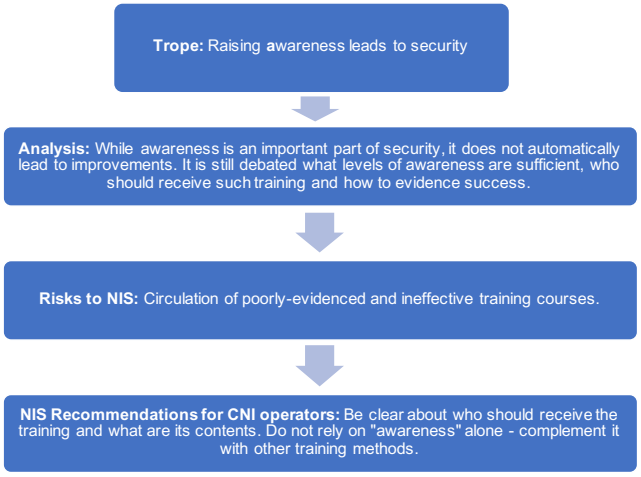

Figure 6: Analysis of the OT Security trope: Raising awareness leads to security.

4.3 Social practices observed

The following section will turn to social practices of NIS implementation, an uncovered through our qualitative interviews. If behaviors are analyzed through the lens of individual perceptions, motivations and attitudes; both OT security tropes and practices are examined in relation to power, competences, meanings and materials [62]. We show that a nuanced understanding of OT security tropes could contribute to the construction of well-evidenced and context-specific expertise and, ultimately, to the adoption of secure practices. However, as OT security is in the early stage of professionalization, some of the observed practices could, in fact, undermine the case for improvements in security through regulations.

Drawing from previous studies on policy classifications [13, 67]we argue that an empirically based exploratory classification system could be of use to fellow researchers and practitioners. We classified the policies under high-level themes to avoid falling into the trap of a formalistic understanding of law; instead showing that NIS does not happen in vacuum and is shaped by the environment in which it is implemented.

4.3.1 Classification of practices

We propose an exploratory classification of practices enacted as a response to cyber security regulations across critical infrastructures (Table 4). The aim of our exploratory classification is to establish an empirically grounded investigation into the 'actually existing' activities rather than idealized types [68]. As such, we identified four main categories: compliance, workaround, going above and beyond policy remit, and negotiation. We recognize that this is not an exhaustive list but, rather, a call for closer examination of the relations between the stakeholders involved in NIS. We intend that the classification could be further utilized by security researchers and practitioners; i.e. they could verify our categories and add new ones to reflect their experiences.

In creating our classification, we acknowledged previous work conducted in the field. For example, compliance and workarounds are well-researched in cyber security [8, 11, 35, 41, 45, 58, 73], however, rarely from the lens of situated practices [22]. The latter two categories ("going above and beyond policy remit" and "negotiation") received less attention in cyber security scholarship (with a notable exception of Slayton and Clark-Ginsberg [66], Shane [60] and Carr [19]).

Overall, past literature conceptualized compliance and workarounds as one-way transactions, where a policymaker sets the rules and a policy recipient responds to them. Meanwhile, we question this static configuration, demonstrating that in all four categories critical infrastructure operators are not passive recipients of the policy but its active co-creators. Consequently, our analysis is focused on relations which make the acts of policy interpretation and implementation "happen".

4.3.2 Compliance

We understand compliance as "*the act of obeying a formal cyber security policy*". The topic was extensively studied by the security community. For example, Gerber et al. [35] investigated the effectiveness of goal setting and rewards, whereas Safa et al. [58] and Bauer and Bernroider [8] examined employees' attitudes to compliance drawing from the social bond

Table 4: Practices of policy interpretation and implementation in the field of OT security.

	Compliance	Workaround	Going above and beyond policy remit	Negotiation
Security Example	Completing asset discovery as an essential basis for further cyber improvements	OT experts implementing their own security measures, using policy as a "sanity check"	Intelligence sharing through a working group set on the basis of trust and shared terms of reference	Operators giving feedback on Infosec-biased language of self-assessment forms
Insecurity example	Interpreting the scope of NIS self-assessment framework to own advantage, while excluding key OT assets	Senior executives ignoring the need for improvements	Overreliance on the latest 'buzzword' technologies when basic knowledge is missing	Prioritizing business values over public values in policy interpretation (e.g., security at cost of privacy)

theory and the theory of reasoned action. Yet, we observe that compliance is not limited to a mere acceptance of the policy (expressed by, for example, a positive attitude to it), but it involves a degree of interpretation.

The NIS Regulations are written in a top-down manner; therefore, they are not specific to CNI sectors. At the time of writing, the only sector-specific documents were regulators' guidelines on completing self-assessment forms. In the eyes of critical infrastructure operators, NIS requires the operators to manage assets which not only previously lacked regulations in terms of security, but also lacked adequate procedures in other operational areas. As such, some participants admitted that they need to *"get the basics right before thinking about expensive silver bullets"* [P01]. In order to improve the basics of security, CNI operators ought to record their assets, decide which ones to deem critical and, then, establish procedures for management and monitoring: *"CNIs don't necessarily understand their assets. So, the water industry, for instance, might have tens of thousands of assets distributed over, 200, 300 square km. Do they know everything about every one of those assets? Not necessarily because some of them might have been put in 50, 60 years ago. They might have dropped off an asset list sometime. They might have come back on. It might have been refreshed but left there. Who knows? And they are finding out that the work, that a discovery piece in their asset management is pretty huge"* [P01]

How does one know what counts as a critical asset? We observed that this decision usually depends on the security manager's competences: what if an IT-trained practitioner included only enterprise IT, excluding cyber-physical infrastructures from the scope? Furthermore, our analysis shows that the processes also differ depending on the organization type, e.g., participants argued that asset discovery is more challenging in CNIs with geographically dispersed assets, e.g., in the water sector. Finally, we argue that understanding of *asset criticality* can be constructed as a way to advance own career: a security manager could be interpreting the scope of NIS self-assessment framework to achieve a good score, while excluding assets which cannot be easily secured. One participant remarked: *"As the self-assessment form is subjective, it is a reflection of mindsets rather than cyber maturity, e.g. some companies are adding physical security*[1] *stuff in their scope and, therefore scoring themselves higher."* [P27].

We link these compliance practices to the trope that "awareness leads to security". We suggest asking: who should be aware of what? What assumptions are made about the current awareness of policymakers and CNI operators? Should policymakers be aware of sectoral specifics so they can write better guidelines? Should security managers (especially if their role or a whole field is new) be assumed to correctly assess the policy scope? We recommend that practitioners pay continuous attention to the idea of "translation" across IT and OT as well as across the sectors to improve their capabilities of policy formulation and interpretation.

4.3.3 Workarounds

Workarounds are "*circumventions of a cyber security policy, which do not explicitly address its problems*". Like compliance, workarounds received considerable attention from the researchers, especially as they tie into the idea of usability [11, 73] Kirlappos et al. [41] introduced the term "shadow security" to describe employees' unofficial security measures (some of them of questionable efficacy) devised to ensure their day-to-day work goals are achieved. Koppel et al. [43] argued that understanding workarounds requires not only an analysis of technical rules, but also interviews and observations of key informants. In our classification of practices as workarounds, we drew from social scientific understanding of the term [17], identifying actions which evade security policies in a non-confrontational manner. Through avoiding confrontation and applying their own definitions of "appropriate and proportionate measures", NIS stakeholders are devoid of an opportunity to negotiate the scope of the policy.

In the context of NIS, some operators were known to implement their own security improvement plans, using NIS as a "sanity check". One of the energy regulators argued that this is a welcome practice since the policy was written in a basic and generic way: *"There are people who are more confident, or have a different attitude to risk perhaps, and will have their own views about what is the right thing to do in their organization, and they might use NIS as a kind of sanity check, a checklist to see how they compare with it. But their real logic, decision-making will be based on their expert knowledge of what they think is the best thing to do in their circumstances, and they won't blindly follow NIS"* [P02].

Operators could also use workarounds to avoid implementing security measures without the need to openly criticize

[1] CNI employees traditionally differentiate between cyber security (related to the protection of personnel and equipment from malicious incidents using digital technologies), physical security (related to the protection of personnel and equipment from malicious incidents) and safety (related to the protection of personnel and equipment from accidents).

policy, e.g.: *"I didn't enjoy being a CISO because it was always going into the board saying: "You need to spend money", and the board said "Well, why? Prove it, show me metrics, show me reasons", and I can scare them with regulations, but it was never a very scientific question, it was always a bit finger in the air and, "This is what happens if we don't do it, but it might not because we might not get hit""* [P10]. We note that as the core requirement of NIS is responding in an "appropriate and proportionate" manner, the policy does not prescribe risk assessment methodologies or security budgets, leaving the decision what (not) to secure to the operators.

We link the above "workaround" to the trope "separations means security". Here we reiterate the point, that "appropriate and proportionate" interpretation of NIS cannot be simply assumed as senior decision makers in CNIs might not have the expertise in the state-of-the-art attack methods. We also state that relying on outdated measured is not only linked to the lack of knowledge, but also to organizational hierarchies: board members might circumvent the policy if it is tied to activities, they are not willing to take part in. We cannot ignore the dimensions of power relations present in workaround practices. To better understand how practitioners, construct the notions of "risk" and "appropriate measures", we recommend further research asking the following questions: How is this knowledge negotiated between the board, a CISO and other employees? How do practitioners know what is "proportionate and appropriate"?

4.3.4 Going above and beyond policy remit

Across the responses to NIS, we noticed that the ambitions of some critical infrastructure operators exceeded the policy requirements. We call this category "going above and beyond the policy remit". As OT cyber security policies are new, we did not identify any relevant past research related to this concept. However, we noted that there is a considerable amount of grey literature on "industry best practices" (e.g., [1, 34]). While these reports might be detailed and informative, they lack rigor to be treated as evidence for policymaking.

We identified that certain CNI operators formed working groups to share progress on NIS and establish a whole-sector benchmark. We claim that these practices are examples of reconfigurations of power and competence, where the operators are able to elevate their status through co-operation and sharing capabilities. The existence of working groups questions the notion of policy implementation as a one-way, passive activity. Their evolution will be interesting to observe, especially as many of CNIs for-profit companies and competitors.

As participants reported, working groups were not required by the regulators, therefore they tend to be industry-led: *"So, the working group is something has been going on for years now. We [regulators] are not permanent members. We were invited, of course, to be part, but this is a closed forum for operators that is running for years for them to share and it's not only about cyber but also about other topics as well to share and to experience"* [P03]. Nevertheless, working groups are not necessarily uniformly effective. Participants remarked that the key to success are: the basis of trust, shared terms of reference and secure storage of confidential data.

An example of a high ambition which does not lead to security improvements is overreliance on the latest 'buzzword' technologies when basic knowledge of security is missing. We noted participants' fears that some operators can be tempted to neglect basic improvements in favor of asset upgrades which they argue as "due to be replaced". Regulators reported that the key part of their role to differentiate between legitimate security improvements and costly innovations for their own sake: *"We want a highly resilient network, so that implies that you replace these assets before they stop working, and there's some subjectivity when that should be. So, there's an argument that operators put forward is, we should replace those assets a bit sooner than previously forecasted and at the same time we can upgrade the cyber security. So that potentially saves them some money, but it's hard to draw out the separation sometimes between the cyber security arguments and the physical lifetime of the assets, but there are big sums of money, hundreds of millions."* [P02].

Consequently, we identify that the practices of "going above and beyond policies" are at risk of falling for the "IIOT is inevitable" trope. We recommend that security practitioners are cautious of the promises made by the manufacturers of innovative technologies. IIoT, machine learning, and "essential upgrades" are not necessarily inevitable. Furthermore, the funding mechanisms of critical infrastructures innovations in the field of security ought to receive a closer scrutiny.

4.3.5 Negotiation

Our final category of Operational Techonology cyber security policy response is negotiation. We define it as a *"collaborative process, where cyber security stakeholders co-create the interpretation and implementation of the policy"*. Negotiations often involve compromising on conflicting priorities. Co-production of cyber security expertise was described by Slayton and Clark-Ginsberg [66] who argued that cyber security expertise is value-laden and it can contribute to "regulatory capture", a situation where regulation serves private interests rather than the public good. Furthermore, Carr [19] analyzed the private-public partnerships forming in the UK and the U.S. Her paper identified a disconnect between the expectations of the public and private sector stakeholders in terms of roles, responsibilities and power. These influential papers are one of the few high-level empirical works in the field of cyber security governance. Here we complement their findings by outlining the details of stakeholders' configurations and practices on the ground.

One example of negotiation is the practice of the operators and regulators working together to improve the language of

NIS guidelines and self-assessment forms. In the following quote, an OT security manager busts the myth that "security measures are the same across the sectors". He reports: *"one of my big bugbears with the OT cyber security policies is that they are info sec driven. I prefer to use the term "cybersecurity" because information isn't the asset. Traditionally, forget the computer systems. I start with something I say to everybody. There are two fundamental differences between information security and OT security. Number one is that the computer system is just another component in the mechanical plant in my world. So, it has no more importance than a pump or a valve. If it breaks, the plant stops working (. . .) So the regulator looked for two water companies to work with them last year to develop NIS into something workable for the water industry. They brought out draft guidance and I sat down with them for a day, and I went through some of the things which just don't work and there's a big difference."* [P26]

In negotiating how to improve security through NIS through the emerging working groups and public-private partnerships, there is a risk that a significant influence of private sector over policy interpretation could lead to prioritizing business values over public values. As the most cyber-mature operators establish close relationships with the regulators, policymakers ought to remain objective and avoid biases during audits and funding competitions. To complement that, CNI operators ought to improve their capabilities in the areas of human and social factors of technology, so they while implementing NIS, they do not compromise on other public values such as privacy, sustainability or equity.

4.4 POLICY RECOMMENDATIONS FOR NIS DIRECTIVE

Based on the analysis of OT security tropes in conjunction with our mapping of policy implementation practices, we proved a set of five policy recommendations for NIS stakeholders in the UK and other European countries. We outline these below mirroring the order of research findings in earlier sections and specifying the target audience for each.

Recommendation 1 (for CNIs operators deciding on improvement plans): Know about and protect yourselves against threats which circumvent air-gapped systems. Check whether alternatives to air-gapping comply with safety standards.

Recommendation 2 (for regulatory bodies overseeing NIS): Align the timescales of innovation funding, regular upgrades and NIS improvement plans. When approving price reviews for network upgrades, seek robust evidence for the claims on the operational benefits of proposed innovations.

Recommendation 3 (for CNI operators responsible for cyber security training): Tie the training to employees' personal concerns to make it relatable and interesting. Do not rely on "awareness" alone - complement it with other training methods. Above all, place "awareness" in the usability context of daily work; i.e. plant supervisors have different concerns to admin staff.

Recommendation 4 (for all stakeholders) Practitioners should pay continuous attention to the idea of "translation" across IT and OT as well as across the sectors to improve their capabilities of policy formulation and interpretation. This will ensure that the scope and latter auditing of NIS pertains both OT and IT and that the improvements are tailored to each system.

Recommendation 5 (for all stakeholders) We recommend that security practitioners ought to improve their capabilities in the areas of human and social factors of technology, so they while implementing NIS, they do not compromise on other public values such as privacy, sustainability or equity.

5 Conclusions

The Network and Information Systems Security (NIS) Directive is the first European-scale attempt to establish a high standard of cybersecurity among the operators of critical infrastructures. In order to understand whether it is likely to bring about a meaningful organizational change and avoid becoming a tick-box exercise, we interviewed 30 UK-based cyber security practitioners inquiring about their experiences of policy implementation.

Our analysis found that the emerging field of Operational Technology (OT) Security is yet to formulate norms, standards and career trajectories. We ought to be careful that "OT security tropes" are appropriately scrutinized before serving as policy advice. Furthermore, our study proposed a classification of cyber security practices which maps the diversity of policy responses to NIS. We analyzed OT security practices through the lens of OT security tropes to indicate whether they could lead to more security or insecurity. As such, we observed that the process of NIS implementation is a two-way exchange. We provided empirical examples of the practices of negotiation and going above and beyond policy remit which illustrate this point. Similarly, we argue that compliance with NIS might not be reduced to a tick-box exercise if practitioners are reflective about "OT security tropes" circulating in the field. Practices most likely to bring about meaningful organizational change are appropriately situated in the OT and sector-specific context and aligned with cross-cutting public values (e.g. security, privacy, sustainability and equity).

From a research point of view, our findings recommend that the funding mechanisms of CNI innovations in the field of security ought to receive closer scrutiny, and that further research should be done to better understand how practitioners construct the notions of "risk" and "appropriate and proportionate measures".

Acknowledgments

This work was supported by RITICS grant "How many shades of NIS? Understanding Organizational Cybersecurity Cultures and Sectoral Differences".

References

[1] 12 Best Cybersecurity Practices in 2020. https://www.ekransystem.com/en/blog/best-cyber-security-practices. Accessed: 26-02-2020.

[2] Directive (EU) 2016/1148 of the european parliament and of the council of 6 july 2016 concerning measures for a high common level of security of network and information systems across the union. *OJ*, L 194, 19-07-2016.

[3] Zauwiyah Ahmad, Mariati Norhashim, Ong Thian Song, and Liew Tze Hui. A typology of employees' information security behaviour. In *2016 4th International Conference on Information and Communication Technology (ICoICT)*, pages 1–4. IEEE, 2016.

[4] Claudia Aradau. Security that matters: Critical infrastructure and objects of protection. *Security dialogue*, 41(5):491–514, 2010.

[5] Helder Aranha, Massimiliano Masi, Tanja Pavleska, and Giovanni Paolo Sellitto. Enabling security-by-design in smart grids: An architecture-based approach. In *2019 15th European Dependable Computing Conference (EDCC)*, pages 177–179. IEEE, 2019.

[6] Maria Bada, Angela M Sasse, and Jason RC Nurse. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*, 2019.

[7] Rosaline S Barbour. Checklists for improving rigour in qualitative research: a case of the tail wagging the dog? *Bmj*, 322(7294):1115–1117, 2001.

[8] Stefan Bauer and Edward WN Bernroider. From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, 48(3):44–68, 2017.

[9] Bernadette Bensaude Vincent. The politics of buzzwords at the interface of technoscience, market and society: The case of 'public engagement in science'. *Public understanding of science*, 23(3):238–253, 2014.

[10] Bird & Bird. Developments on nis directive in eu member states. Technical report, 2020.

[11] Jim Blythe, Ross Koppel, and Sean W Smith. Circumvention of security: Good users do bad things. *IEEE Security & Privacy*, 11(5):80–83, 2013.

[12] John M Blythe, Lynne Coventry, and Linda Little. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On Usable Privacy and Security (SOUPS) 2015)*, pages 103–122, 2015.

[13] Geoffrey C Bowker and Susan Leigh Star. *Sorting things out: Classification and its consequences*. MIT press, 1999.

[14] Ross Boyd and Robert J Holton. Technology, innovation, employment and power: Does robotics and artificial intelligence really mean social transformation? *Journal of Sociology*, 54(3):331–345, 2018.

[15] Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson. The industrial internet of things (iiot): An analysis framework. *Computers in Industry*, 101:1–12, 2018.

[16] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[17] David Campbell. Policy workaround stories are valuable evaluative indicators: but should they be told? *American Journal of Evaluation*, 32(3):408–417, 2011.

[18] Catarina Araya Cardoso, Jacopo Torriti, and Mate Lorincz. Making demand side response happen: A review of barriers in commercial and public organisations. *Energy Research & Social Science*, 64:101443, 2020.

[19] Madeline Carr. Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1):43–62, 2016.

[20] Madeline Carr and Leonie Maria Tanczer. Uk cybersecurity industrial policy: an analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, 3(3):430–444, 2018.

[21] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388, 2016.

[22] Myriam Dunn Cavelty. Cybersecurity research meets science and technology studies. *Politics and Governance*, 6(2):22–30, 2018.

[23] Weiping Cheng, Hongji Fang, Gang Xu, and Meijun Chen. Using scada to detect and locate bursts in a long-distance water pipeline. *Water*, 10(12):1727, 2018.

[24] Yulia Cherdantseva, Pete Burnap, Andrew Blyth, Peter Eden, Kevin Jones, Hugh Soulsby, and Kristan Stoddart. A review of cyber security risk assessment methods for scada systems. *Computers & security*, 56:1–27, 2016.

[25] Jennifer Chubb, Jasper Montana, Jack Stilgoe1, Andy Stirling, and James Wilsdon. A review of recent evidence on the governance of emerging science and technology. Technical report, Wellcome Trust, 11 2018.

[26] Sauvik Das, Laura A Dabbish, and Jason I Hong. A typology of perceived triggers for end-user security and privacy behaviors. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[27] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS) 2014)*, pages 143–157, 2014.

[28] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. *arXiv preprint arXiv:1808.05096*, 2018.

[29] AC Alessandro Di Pinto, Younes Dragoni, and Andrea Carcano. Triton: The first ics cyber attack on safety instrument systems. In *Proc. Black Hat USA*, pages 1–26, 2018.

[30] Yvonne Dittrich. What does it mean to use a method? towards a practice theory for software engineering. *Information and Software Technology*, 70:220–231, 2016.

[31] Jens Ivo Engels. *Key Concepts for Critical Infrastructure Research*. Springer, 2018.

[32] Sandra L Faulkner and Stormy P Trotter. Data saturation. *The international encyclopedia of communication research methods*, pages 1–2, 2017.

[33] Sylvain Frey, Awais Rashid, Alberto Zanutto, Jerry Busby, and Karolina Follis. On the role of latent design conditions in cyber-physical systems security. In *Proceedings of the 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems*, pages 43–46, 2016.

[34] GE. An executive guide to cyber security for operational technology. Technical report, 2017.

[35] Nina Gerber, Ronja McDermott, Melanie Volkamer, and Joachim Vogt. Understanding information security compliance-why goal setting and rewards might be a bad idea. In *HAISA*, pages 145–155, 2016.

[36] Antonios Gouglidis, Benjamin Green, Jeremy Busby, Mark Rouncefield, David Hutchison, and Stefan Schauer. Threat awareness for critical infrastructures resilience. In *2016 8th International Workshop on Resilient Networks Design and Modeling (RNDM)*, pages 196–202. IEEE, 2016.

[37] Julie M Haney and Wayne G Lutters. "it's scary... it's confusing...it's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS) 2018)*, pages 411–425, 2018.

[38] Wayne Harrop and Ashley Matteson. Cyber resilience: A review of critical national infrastructure and cybersecurity protection measures applied in the uk and usa. In *Current and Emerging Trends in Cyber Operations*, pages 149–166. Springer, 2015.

[39] Chris Jay Hoofnagle, Bart van der Sloot, and Frederik Zuiderveen Borgesius. The european union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1):65–98, 2019.

[40] $(ISC)^2$. Strategies for building and growing strong cybersecurity teams. Technical report, 2019.

[41] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. " shadow security" as a tool for the learning organization. *ACM SIGCAS Computers and Society*, 45(1):29–37, 2015.

[42] Simon C Kitto, Janice Chesters, and Carol Grbich. Quality in qualitative research. *Medical journal of Australia*, 188(4):243–246, 2008.

[43] Ross Koppel, Sean W Smith, Jim Blythe, and Vijay H Kothari. Workarounds to computer access in healthcare organizations: you want my password or a dead patient? *ITCH*, 15(4):215–220, 2015.

[44] PJ Lavrakas. Key informant. *En Encyclopedia of Survey Research Methods*, page 2455, 2008.

[45] Chunghun Lee, Choong C Lee, and Suhyun Kim. Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security*, 59:60–70, 2016.

[46] John Lindström, Petra Viklund, Tideman Fredrik, Hällgren Berndt, and Elvelin Jonny. Oh, no–not another policy! oh, yes-an ot-policy! In *52nd CIRP Conference on Manufacturing Systems (CMS), Ljubljana, Slovenia, June 12-14, 2019*, volume 81, pages 582–587, 2019.

[47] Martin Lundgren and Erik Bergström. Security-related stress: A perspective on information security risk management. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–8. IEEE, 2019.

[48] Erik Skov Madsen, Arne Bilberg, and D Grube Hansen. Industry 4.0 and digitalization call for vocational skills, applied industrial engineering, and less for pure academics. In *Proceedings of the 5th P&OM World Conference, Production and Operations Management, P&OM*, 2016.

[49] Leandros Maglaras, George Drivas, Kleanthis Noou, and Stylianos Rallis. Nis directive: The case of greece. *EAI Endorsed Transactions on Security and Safety*, 4(14), 2018.

[50] Shrirang Mare, Mary Baker, and Jeremy Gummeson. A study of authentication in daily life. In *Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016)*, pages 189–206, 2016.

[51] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert. The new eu cybersecurity framework: The nis directive, enisa's role and the general data protection regulation. *Computer Law & Security Review*, 35(6):105336, 2019.

[52] Bryan Marshall, Peter Cardon, Amit Poddar, and Renee Fontenot. Does sample size matter in qualitative research?: A review of qualitative interviews in is research. *Journal of computer information systems*, 54(1):11–22, 2013.

[53] Fabio Massacci, Raminder Ruprai, Matthew Collinson, and Julian Williams. Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers. *IEEE Security & Privacy*, 14(3):52–60, 2016.

[54] Clark A Miller and Sheila Jasanoff. States of knowledge: The co-production of science and social order, 2004.

[55] Chaim Noy. Sampling knowledge: The hermeneutics of snowball sampling in qualitative research. *International Journal of social research methodology*, 11(4):327–344, 2008.

[56] Qais Saif Qassim, Norziana Jamil, Maslina Daud, Ahmed Patel, and Norhamadi Ja'affar. A review of security assessment methodologies in industrial control systems. *Information & Computer Security*, 2019.

[57] Awais Rashid, Joseph Gardiner, Benjamin Green, and Barnaby Craggs. Everything is awesome! or is it? cyber security risks in critical infrastructure. In *International Conference on Critical Information Infrastructures Security*, pages 3–17. Springer, 2019.

[58] Nader Sohrabi Safa, Rossouw Von Solms, and Steven Furnell. Information security policy compliance model in organizations. *computers & security*, 56:70–82, 2016.

[59] P Shakarian, J Shakarian, and A Ruef. Attacking iranian nuclear facilities: Stuxnet. *Introduction to cyberwarfare: A multidisciplinary approach*, pages 223–239, 2013.

[60] Peter M Shane. Cybersecurity policy as if ordinary citizens mattered: The case for public participation in cyber policy making. *Isjlp*, 8:433, 2012.

[61] James Shires. Enacting expertise: Ritual and risk in cybersecurity. *Politics and Governance*, 6(2):31–40, 2018.

[62] Elizabeth Shove, Mika Pantzar, and Matt Watson. *The dynamics of social practice: Everyday life and how it changes*. Sage, 2012.

[63] Elizabeth Shove and Frank Trentmann. *Infrastructures in practice: the dynamics of demand in networked societies*. Routledge, 2018.

[64] Meha Shukla, Shane D Johnson, and Peter Jones. Does the NIS implementation strategy effectively address cyber security risks in the uk? In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, pages 1–11. IEEE, 2019.

[65] Molly J Simis, Haley Madden, Michael A Cacciatore, and Sara K Yeo. The lure of rationality: Why does the deficit model persist in science communication? *Public Understanding of Science*, 25(4):400–414, 2016.

[66] Rebecca Slayton and Aaron Clark-Ginsberg. Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation & Governance*, 12(1):115–130, 2018.

[67] Kevin B Smith. Typologies, taxonomies, and the benefits of policy classification. *Policy Studies Journal*, 30(3):379–395, 2002.

[68] Kevin B Smith. Typologies, taxonomies, and the benefits of policy classification. *Policy Studies Journal*, 30(3):379–395, 2002.

[69] Kristan Stoddart. Uk cyber security and critical national infrastructure protection. *International Affairs*, 92(5):1079–1105, 2016.

[70] Holger Stritzel. Security, the translation. *Security Dialogue*, 42(4-5):343–355, 2011.

[71] Lucy Suchman. Embodied practices of engineering work. *Mind, Culture, and activity*, 7(1-2):4–18, 2000.

[72] Lucy Suchman, Dominik Gerst, and Hannes Krämer. " if you want to understand the big issues, you need to understand the everyday practices that constitute them." lucy suchman in conversation with dominik gerst & hannes krämer. In *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, volume 20, 2019.

[73] Rogier Woltjer. Workarounds and trade-offs in information security–an exploratory study. *Information & Computer Security*, 2017.

[74] Alberto Zanutto, Benjamin Oliver Shreeve, Karolina Follis, Jeremy Simon Busby, and Awais Rashid. The shadow warriors: In the no man's land between industrial control systems and enterprise it systems. 2017.

[75] Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin, and Hamdullah Nejat Basim. Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, pages 1–16, 2020.

A Codebook

Below are given per theme, the individual codes reported on in this paper, together with a description of their meaning, and exemplary quotes.

A.1 Practices

Compliance, secure

Description: The act of obeying a formal cyber security policy likely to improve security.

Example: "CNIs don't necessarily understand their assets, per se. So, the water industry, for instance, might have tens of thousands of assets distributed over, 200, 300 square km. Do they know everything about every one of those assets? Not necessarily because some of them might have been put in 50, 60 years ago. They might have dropped off an asset list sometime. They might have come back on. It might have been refreshed but left there. Who knows? And they are finding out that the work, that a discovery piece in their asset management is pretty huge"

Compliance, insecure

Description: The act of obeying a formal cyber security policy likely to deteriorate security.

Example: "As the self-assessment form is subjective, it is a reflection of mindsets rather than actual cyber maturity, for example some companies are adding physical security stuff in their scope and, therefore scoring themselves higher

Workaround, secure

Description: Circumventions of a cyber security policy which do not explicitly address its problems; likely to improve security.

Example: ""There are people who are more confident, or have a different attitude to risk perhaps, and will have their own views about what is the right thing to do in their organization, and they might use NIS as a kind of sanity check, a checklist to see how they compare with it. But their real logic, decision-making will be based on their expert knowledge of what they think is the best thing to do in their circumstances, and they won't blindly follow NIS""

Workaround, insecure

Description: Circumventions of a cyber security policy which do not explicitly address its problems; likely to deteriorate security.

Example: "I didn't enjoy being a CISO because it was always going into the board saying: "You need to spend money", and the board were, like, "Well, why? Prove it, show me metrics, show me reasons", and I can scare them with regulations, but it was never a very scientific question, so to speak, it was always a bit finger in the air and, "This is what happens if we don't do it, but it might not because we might not get hit"

Above and Beyond, secure

Description: The act of exceeding the policy requirements; likely to improve security.

Example: "So, the working group is something has been going on for years now. We [regulators] are not permanent members. We were invited, of course, to be part, but this is a closed forum for operators that is running for years for them to share and it's not only about cyber but also about other topics as well to share and to experience"

Above and Beyond, insecure

Description: The act of exceeding the policy requirements; likely to deteriorate security.

Example: ""We want a highly resilient, highly available network, so that implies that you replace these assets before they stop working, and there's some subjectivity when that should be. So, there's an argument that operators put forward is, well, perhaps we should replace those assets a bit sooner than previously forecasted and at the same time we can upgrade the cybersecurity of the sensors or activators within these devices. So that potentially saves

them some money, but it's hard to draw out the separation sometimes between the cybersecurity arguments and the physical lifetime of the assets, but there are big sums of money"" hundreds of millions.""

Negotiation, secure

Description: Collaborative process, where cyber security stakeholders co-create the interpretation and implementation of the policy; likely to improve security.

Example: "one of my big bugbears with the OT cybersecurity policies is that they are very info sec driven. That's why I prefer to use the term "cybersecurity" because information isn't the asset. Traditionally, forget the computer systems. I start with something I say to everybody. There are two fundamental differences between information security and cybersecurity, OT security. Number one is that the computer system is just another component in the mechanical plant in my world. So, it has no more importance than a pump or a valve or whatever. If it breaks, the plant stops working (. . .) So the regulator looked for two water companies to work with them last year to develop NIS into something workable for the water industry. They brought out draft guidance and I sat down with them for a day, and I went through some of the things which just don't work and there's a big difference."

Negotiation, insecure

Description: Collaborative process, where cyber security stakeholders co-create the interpretation and implementation of the policy; likely to deteriorate security.

Example: "if you have several suppliers, you can actually have competitive discussions with the suppliers. If you actually use one supplier only, you don't have that anymore. One of the problems we're having in the railways on the signalling side is that we're having less and less suppliers and so the costs are spiralling because the supplier knows we don't have any other options."

A.2 Clichés

Separation means security

Description: Comments on air-gapping.

Example: "When you're talking to the board and they say, "We don't need to worry about security because our production facility is airgapped", there is only one place which is air gapped and that is Battlestar Galactica!"

IIOT is inevitable

Description: Comments on the trajectory and pace of innovation.

Example: "We're facing the problem of IIOT arriving. When we did the self-assessment, everyone was using very traditional industrial control systems. In that time in the last six months, we've all started adopting IIOT and it's going to get worse. So, it's a big change and it's one that's very much on everyone's radar including mine"

Solutions are the same across sectors

Description: Comments on sectoral differences and similarities

Example: "the tech basis of cyber is the same across the sectors"

Raising awareness leads to security

Description: Comments on the value of awareness raising activities.

Example: "General population can't rationalize. They can worry. So why would you want to worry a population? Is it beneficial for society to know of all the things that bad people want?"

A.3 Participants

Background

Description: Participants' education and previous roles.

Example: "worked in cyber security back when there was no such thing as cyber security"

Talk

Description: Discourses of participants.

Example: "Virtually, you could look at every outcome in the self assessment framework and have a debate about whether you've met it or not, purely on the basis of what sort of attacks do we expect to defend against. The framework doesn't take a position on that. So when everything's subjective, the decisions are made, are all largely made ultimately on personal opinions and it's hard to summarize, hard to understand from that just what attacks they are designed to be resilient against and what they aren't. Whereas if you have a standards based approach, standards on their own aren't the full solution, but I think they're part of the solution. Things like the [government cyber security] standard, which government has promoted. I don't know if you're aware of that."